IT Security for Industrial Control Systems

Joe Falco, Keith Stouffer, Albert Wavering, Frederick Proctor
Intelligent Systems Division
National Institute of Standards and Technology (NIST)
Gaithersburg, MD

Email: (joseph.falco@nist.gov, keith.stouffer@nist.gov, albert.wavering@nist.gov, frederick.proctor@nist.gov)

In coordination with the Process Control Security Requirements Forum (PCSRF)
(http://www.isd.mel.nist.gov/projects/processcontrol/)

Abstract

The National Institute of Standards and Technology (NIST) is working to improve the information technology (IT) security of networked digital control systems used in industrial applications. This effort is being carried out through the Process Control Security Requirements Forum (PCSRF), an industry group organized under the National Information Assurance Program (NIAP). The PCSRF is working with security professionals to assess the vulnerabilities and establish appropriate strategies for the development of policies to reduce IT security risk within the U.S. process controls industry. The outcome of this work will be the development and dissemination of best practices and ultimately Common Criteria, ISO/IEC 15408 based security specifications that will be used in the procurement, development, and retrofit of industrial control systems. In support of this work this paper addresses the computer control systems used within process control industries, their similarities, and network architectures. A generic set of networking system architectures for industrial process control systems is presented. The vulnerabilities associated with these systems and the IT threats these systems are exposed to are also presented along with a discussion of the Common Criteria and its intended use for these efforts. The current status as well as future efforts of the PCSRF are also discussed.

Introduction

The National Institute of Standards and Technology (NIST), Intelligent Systems Division of the Manufacturing Engineering Laboratory is working with the NIST Information Technology Laboratory and the NIST Electrical and Electronics Engineering Laboratory to improve the IT security of networked digital control systems used in industrial applications. This effort is being carried out through the Process Control Security Requirements Forum (PCSRF), an industry group organized under the National Information Assurance Program (NIAP). NIAP is a joint effort between the NIST and the National Security Agency (NSA). As part of the Critical Infrastructure Protection Program, NIST and NSA are working to provide technical support and guidance to industry to improve the Nation's security posture. The outcome of this work will be the development and dissemination of best practices and ultimately security specifications that will be used in the procurement, development, and retrofit of industrial control systems.

The Process Control Security Requirements Forum (PCSRF) is a working group comprising representative organizations from the various sectors that make up the U.S. Process Control Industry and the vendors that design, produce, and/or integrate components and systems for the industry. The PCSRF is working with security professionals to assess the vulnerabilities and establish appropriate strategies for the development of policies and countermeasures that the U.S. process controls industry would employ through a combination IT and non-IT mechanisms to reduce residual risk to an acceptable level. The Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, is being used to document the results of this effort in the form of Common Criteria Protection Profile security specifications. Primary focus area of the group to improve the IT security of the computer control systems used in process industries, including electric utilities, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals & mining with an emphasis on industries considered to be part of the Nation's Critical Infrastructure.

This paper discusses the computer control systems used within process control industries, their similarities, and network architectures. A generic set of network system architectures for industrial process control systems is presented. The IT threats these systems are exposed to are also presented along with a discussion of the Common Criteria and its intended use for these efforts. The current status as well as future efforts of the PCSRF are also discussed.

Process Control Computer Systems

Real-time computer control systems used in process control applications have many characteristics that are different than traditional information processing systems used in business applications. Foremost among these is design for efficiency and time-critical response. Security is generally not a strong design driver and therefore tends to be bypassed in favor of performance. Computing resources (including CPU time and memory) available to perform security functions tend to be very limited. Furthermore, the goals of safety and security sometimes conflict in the design and operation of control systems.

Commercial equipment and materials are identified, in order to adequately specify certain systems. In no case does such identification imply recommendation of endorsement by the National Institute of Standards and Technology, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

Digital industrial control systems can be either process-based or discrete-based. Process-based controls [1] are used to control a continuous process such as fuel or steam flow in a power plant or petroleum in a refinery. Discrete-based controls (otherwise known as batch controls) control discrete parts manufacturing or "batches" of material in a chemical plant. Both utilize the same types of control systems, sensors, and networks. While efforts of the PCSRF are currently geared toward continuous processing systems, results will likely be applicable to discrete based systems.

The key control components of an industrial control system, including the control loop, the human - machine interface (HMI), and remote diagnostics and maintenance utilities, are shown in Figure 1. A control loop consists of sensors for measurement, control hardware, process actuators, and communication of measurement variables. Measurement variables are transmitted to the controller from the process sensors. The controller interprets the signals and generates corresponding control signals that it transmits to the process actuators. Process changes result in new sensor signals, identifying the state of the process, to again be transmitted to the controller. The human - machine interface allows a control engineer or operator to configure set points, control algorithms and parameters in the controller. The HMI also provides displays of process status information, including alarms and other means of notifying the operator of malfunctions. Diagnostic and maintenance tools, often made available via modem and Internet enabled interfaces, allow control engineers, operators and vendors to monitor and change controller, actuator, and sensor properties from remote locations. A typical industrial system contains a proliferation of control loops, HMIs and Remote Diagnostics and Maintenance tools built on an array of network protocols. Supervisory level loops and lower level loops operate continuously over the duration of a process at cycle times ranging on the order of minutes to milliseconds.

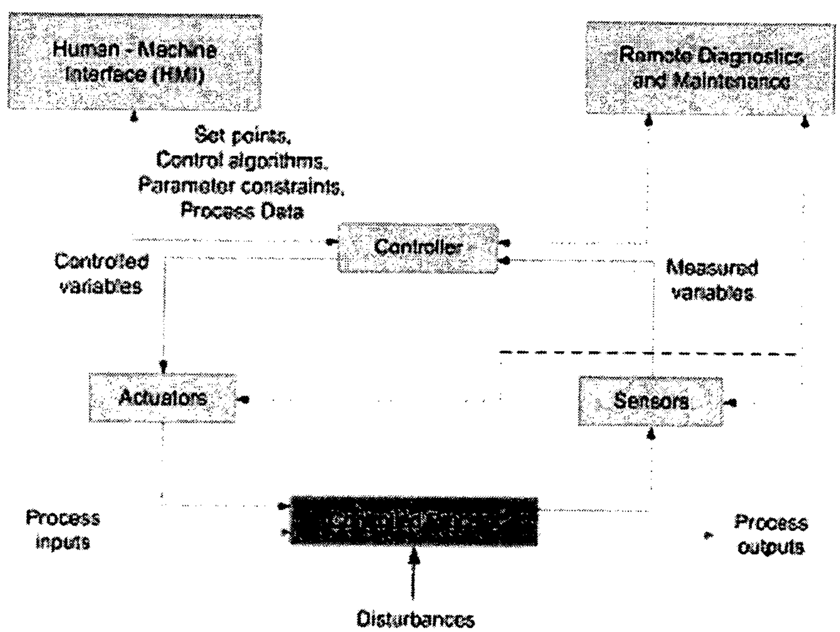

Figure 1 Key Control Components

In a large enterprise, there may be several geographically distributed industrial plants. Enterprise business operations can access plant information over the Internet or in some cases over a wide area network (WAN). The local area network (LAN) of a processing plant services all of the operations within the plant while the actual control system of the plant sits on a somewhat isolated peer-to-peer network. The systems at these levels can be categorized into two types of supervisory based control schemes, Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition Systems (SCADA). DCS are used to control large, complex processes such as power plants, refineries, and chemical plants typically at a single site. SCADA are used to control more dispersed assets where centralized data acquisition is as important as control. Distribution operations including water systems, gas pipelines, and electrical lines use SCADA.

PCSRF members have constructed diagrams of typical DCS and SCADA based control system network architectures derived from industrial plant visits, review of technical documents and workshop based discussions. Generic industrial control system network architectures are shown for both DCS and SCADA based control schemes in Figures 2 and 3 respectively. A glossary of terms describing the components found in the diagram can be found in the Appendix of this document. A comparison of these diagrams shows that at the higher level of the plant network architectures the plant operations are similar for plants containing either DCS or SCADA systems. At this level, everything resides on a local area network. Components include general purpose workstations, printers, plant database, application servers and domain controllers. Communication outside the plant is typically established via a firewall to the Internet or a wide area network (WAN). Modems are also available, usually to allow remote access to employees working from home or on the road. The DCS and local SCADA components of a plant system typically reside on a peer-to-peer network.

A DCS is comprised of a supervisory layer of control and one to several distributed controllers contained within the same processing plant. The supervisory controller runs on the control server and communicates to its subordinates via a peer-to-peer network. The supervisor sends set points to and requests data from the distributed controllers. The distributed controllers control their process actuators based on requests from the supervisor and sensor feedback for process sensors. These controllers typically use a local field bus to communicate with actuators and sensors eliminating the need of point-to-point wiring between the controller and each device. There are several types of controllers used at the distributed control points of a DCS including machine controllers, programmable logic controllers, process controllers and single loop controllers depending on the application. Many of the distributed controllers on a DCS have the capability to be accessed directly via a modem allowing remote diagnostics and servicing by vendors as well as plant engineers.

A SCADA typically consists of a Central Monitoring System (CMS), contained within the plant and one or more Remote Stations. The CMS houses the Control Server and the communications routers via a peer-to-peer network. The CMS collects and logs information gathered by the remote stations and generates necessary actions for events detected. A remote station consists of either a Remote Terminal Unit (RTU) or a Programmable Logic Controller (PLC) which controls actuators and monitors sensors. Remote stations, typically, have the added capability to be interfaced by field operators via hand held devices to perform diagnostic and repair operations. The communications network is the medium for transporting information between remote

stations and the CMS. This is performed using telephone line, cable, or radio frequency. If the remote site is too isolated to be reached directly via a direct radio signal, a radio repeater is used to link the site.

Process Control Industry Overview

The computer control systems used in process industries, including electric utilities, oil & gas, water, waste, chemicals, pharmaceuticals, pulp & paper, and metals & mining can be divided amongst the usage of either DCS or SCADA technology and implementation depends on the geographic distribution of the operation. Network architectures that encompass processing operations involving the transformation of raw materials into a usable product in a continuous fashion, follow the DCS scenario. On the other hand, the network architectures that encompass distribution operations of the usable products, typically over large distances, follow the SCADA scenario.

The electrical power infrastructure is made up of power generation facilities as well as transmission and distribution grids that create and supply electricity to end-users. Power generation facilities using fossil fuel and hydroelectric turbine/generator systems to produce electricity use DCS. The electric power grid is a highly interconnected and dynamic system consisting of thousands of public and private utilities and rural cooperatives. A SCADA system manages electricity distribution by collecting data from and issuing commands to geographically remote field control stations from a centralized location.

Natural gas, crude, refined petroleum, and petroleum-derived fuels represent Oil and Gas substances. The Oil & Gas infrastructure includes the production holding facilities, refining and processing facilities, and distribution mechanisms (including pipelines, ships, trucks, and rail systems) for such substances. Refining and processing facilities make use of DCS while holding facilities and distribution systems utilize SCADA technology.

The water supply infrastructure encompasses water sources, holding facilities, filtration, cleaning and treatment systems and distribution systems. Like electric, oil and gas, the processing operations use DCS technology while the distribution operations use SCADA technology. A waste water treatment infrastructure is very similar to that of a water supply infrastructure. Chemical, pharmaceutical, pulp and paper, and metals and mining industries primarily fit into the category of processing facility and use DCS technology.

Process Control System Vulnerabilities and IT Threats

IT security [2][3] has not been a significant issue within the process controls community. Systems were designed to meet performance, reliability, safety, and flexibility requirements and were typically physically isolated and based on proprietary hardware and communications. The introduction of Internet based information technology within the process controls industry has increased vulnerabilities to the industry's computer systems. Centralized operation and remote

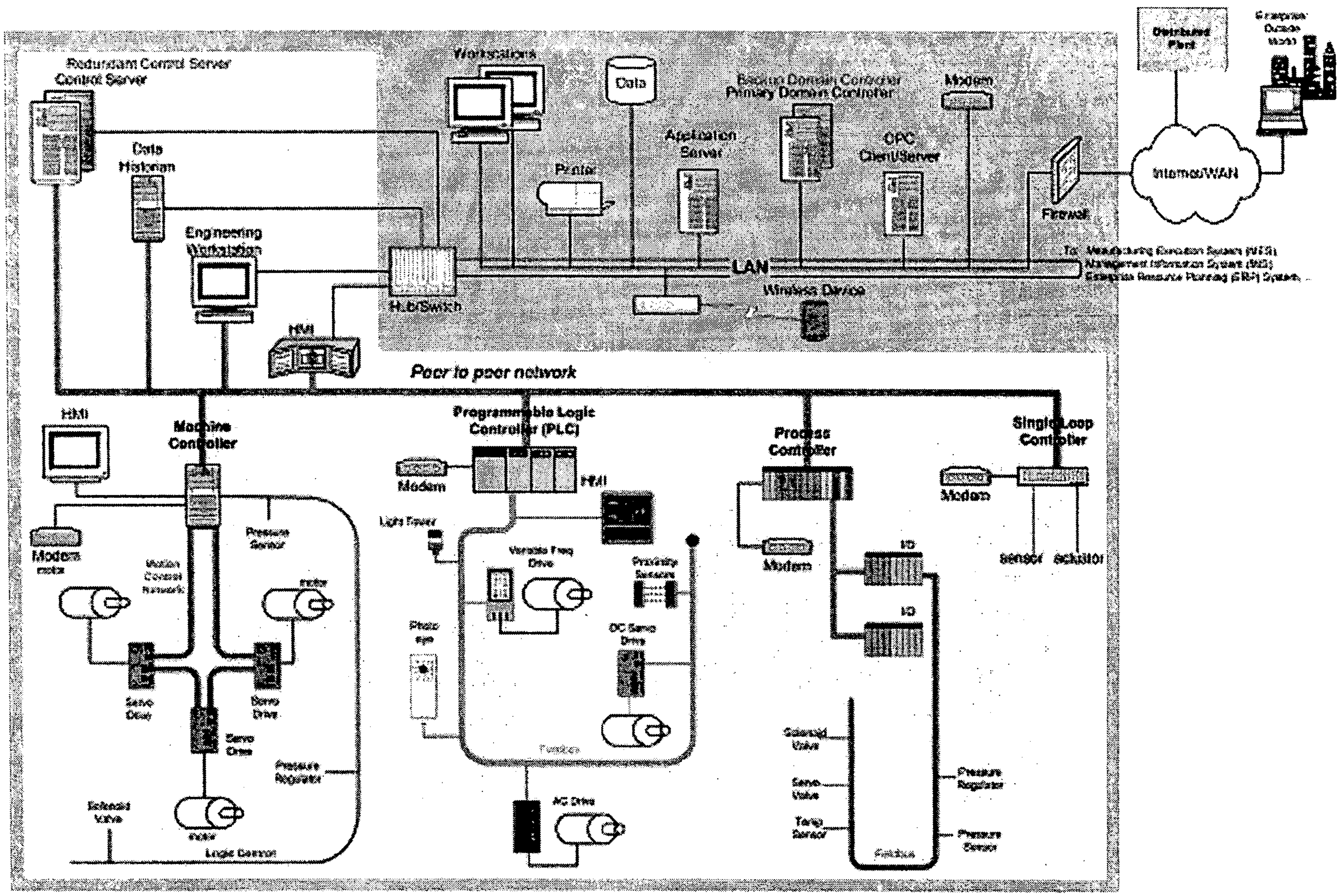

Figure 2: Generic Industrial Control System Network Architecture - DCS

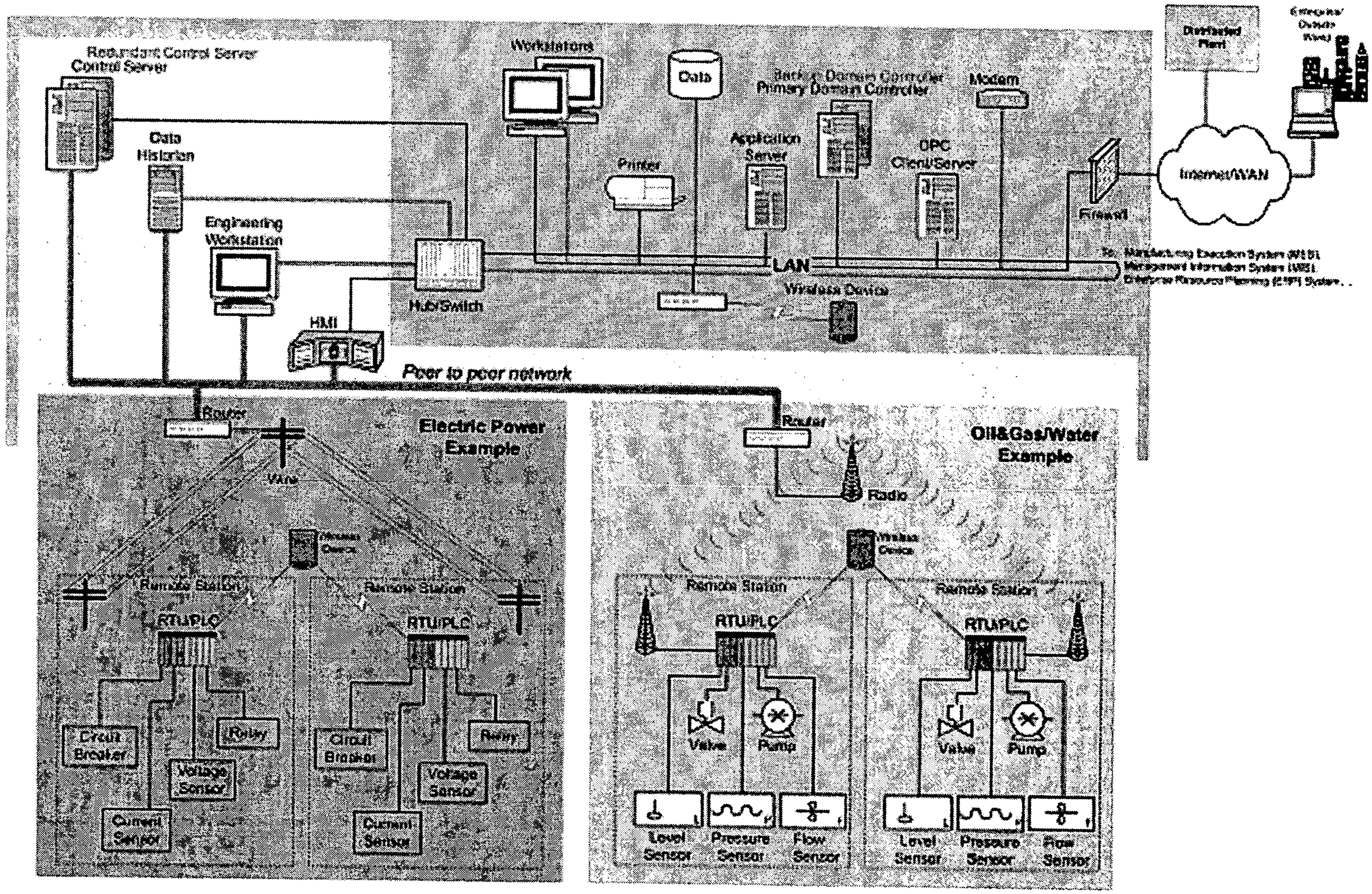

Figure 3: Generic Industrial Control System Network Architecture - SCADA

maintenance of industry systems conducted freely over public telecommunication networks opens the door for threatening organizations to tamper with this critical infrastructure. DCS and SCADA systems that operate on commercial off-the-shelf hardware and software, combined with connections to external networks, allow for simplified invasion and possibly devastation of company production and distribution systems. Threats to these infrastructures could come from numerous sources: hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters. A generalized list of IT threats, extracted from the Common Criteria Toolbox [4], can be found Appendix II.

There are several risks associated with IT threats to industrial control systems. The most consequential risks, those associated with the health and safety of human lives, primarily belong to the industries identified as part of the critical infrastructure. Cyber attacks on energy production and distribution systems including electric, oil, and gas, water treatment and distribution systems as well as on chemical plants containing potentially hazardous substances could endanger public health and safety as well as invoke serious damage to the environment. Attacks on any of the process control industries discussed could result in serious financial implications including loss of production, generation or distribution of a product, compromising of proprietary information and creation of liability issues.

The introduction of Internet based IT and enterprise integration strategies coupled with lack of IT security knowledge has left process control systems vulnerable to cyber based attacks [4-6]. Control networks have been merged with corporate network connections to allow engineers to monitor and control systems from points on the corporate network. IT mechanisms are also in place to allow corporate, decision makers to obtain instant access to critical data. Network architecture modifications, often implemented without a full understanding of the corresponding security risks, can lead to control networks that are only as secure as the corporate network.

Vulnerabilities are dependent on the existing network architectures, IT policies and risks associated with a particular industrial process control system. One initial focus of the PCSRF is to identify and document these vulnerabilities across the industries represented by the PCSRF. These vulnerabilities will be used in the development of best practices and security specifications.

Vulnerabilities are often introduced into process control systems due to the lack of policy. Corporate IT policy can reduce vulnerabilities by mandating conducts such as password usage and maintenance or requirements for connecting modems to the process control system. Vulnerabilities could even exist because of poorly configured IT security equipment. Other vulnerabilities are associated with the public availability of information on widely used open communication protocols, techniques for the interconnection of DCS and SCADA and widely used, commercially available, Internet connectable, toolkits for implementing DCS and SCADA.

Common Criteria Based Approach

The Common Criteria (CC), ISO/IEC 15408 [7], is a meta-standard of criteria and constructs used to develop security specifications in support of the evaluation of products and systems. The

specifications define and characterize the security problem including assumptions about the operational environment, threats that must be encountered and policies that must be enforced. Also characterized is the intended approach to eliminate, minimize or monitor defined threats, and enforce stated policy. The specification defines functional requirements, specifying what the system is to do and assurance requirements, specifying what is done to verify that the system does exactly what it is supposed to. These CC requirements, selected from a catalog of criteria, are independent of technology and implementation. The finished specification is a formal CC Protection Profile (PP) for a product or system. A PP is applied to serve as an acquisition/ procurement vehicle to specify the security requirements of a component or system design or to gauge the security features of available components or systems. A PP can also be applied to verify product compliance both at the component evaluation level and at the system certification level.

Initial PCSRF specifications are being documented using a variation of the CC Protection Profile (PP) methodology of developing security specifications. Rather than working directly within the context of the CC's language and constructs, this effort will focus on developing and documenting requirements using the language of the process control industry operating domains. In turn, this intermediate specification will be translated into one or more CC-compliant protection profiles. This will enable the inclusion of safety critical and performance information in relation to the security aspects of the specification, topics that are not covered by the CC.

During initial information gathering exercises, the PCSRF plans to identify vulnerabilities across the diversities of the participating industry boundaries. Industry specific working groups will define vulnerabilities specific to their process control system based on a minimal set of system functions and capabilities defined by the PCSRF. The results of the individual vulnerability assessments will be analyzed and consolidated, by the PCSRF, into comprehensive statements of vulnerabilities to be used in the development of protection profile(s).

PCSRF Activities

The PCSRF includes representatives from electric power, oil and gas, pulp & paper, water treatment and distribution, and systems integration sectors. This representation comes from both industry as well as organizations such as the EPRI, the American Gas Association (AGA), the Association of Metropolitan Water Agencies (AMWA), the Society of Instrumentation, Systems, and Automation (ISA). Government participation includes NSA, DOE, and NIST. Participation from other industrial process control sectors is also being explored. The PCSRF has contracted a specialist in IT security requirements definition to assist in its efforts, conducted several meetings and established a web site at http://www.isd.mel.nist.gov/projects/processcontrol.

The PCSRF has initiated efforts toward its goals of developing best practices and security specifications for industrial control systems. PCSRF members visited an electric power generation facility, a pulp and paper manufacturing facility, and a manufacturer of industrial control systems. Based on these visits, the review of many technical documents and workshop based discussions, members have constructed diagrams of typical DCS and SCADA based control system network architectures and have developed initial fault/attack trees to examine typical sequences of events needed to cause catastrophic consequences to these systems.

Through interactions with the group and analysis of existing systems, the contracted security consultant is drafting a security profile specification document that defines the security environment, threats, vulnerabilities, and assumptions about a typical systems in the terminology used within the industrial control community. Along with this specification development, the intermediate task of performing vulnerability and threat analysis within the specific sector industries of the PCSRF is being conducted through working groups. Once the security profile specification is drafted, work will begin to translate it into a common set of formal information security requirements (Common Criteria, ISO/IEC 15408, Protection Profiles) and documented best practices for the systems described. Organization based members of the PCSRF are also discussing the future requirements of training and certification to insure the implementation of IT security in process control systems.

Summary

The PCSRF is using the Common Criteria to develop IT security specifications for process control systems. During initial information gathering exercises, the PCSRF plans to identify IT vulnerabilities across the diversities of the participating industry boundaries. Participating industries include: electric utilities, petroleum (oil & gas), water, waste, chemicals, pharmaceuticals, pulp & paper, and metals & mining with an emphasis on industries considered to be part of the Nation's Critical Infrastructure. Industry specific working groups will define vulnerabilities specific to their process control system based on a minimal set of system functions and capabilities defined by the PCSRF. The results of the individual vulnerability assessments will be analyzed and consolidated, by the PCSRF, into comprehensive statements of vulnerabilities to be used in the development of Protection Profile(s). These Protection Profiles will be used in the procurement, development, and retrofit of industrial control systems to improve the Nation's security posture.

Appendix I

Generic Composite Industrial Control System Network Architecture - Glossary

AC Drive – Alternating Current Drive synonymous with *Variable Frequency Drive (VFD).*

Application Server – A computer responsible for hosting applications to user workstations.

Backup Domain Controller – Backup to the Primary Domain Controller.

Control Server – A server hosts the supervisory control system, typically a commercially available application for DCS or SCADA systems, and communicates data between the Peer-to-Peer network and the LAN.

Data – A repository of information that usually holds plant wide information including process data, recipes, personnel data and financial data.

DC Servo Drive – A type of drive that works specifically with servo motors. Transmits commands to the motor and receives feedback from the servo motor's resolver or encoder.

Distributed Control System (DCS) – A supervisory control system typically controls and monitors set points to sub-controllers distributed geographically throughout a factory.

Distributed Plant – A geographically distributed factory that is accessible through the Internet by an enterprise.

Domain Controller - A Windows NT server responsible for managing domain information, such as login IDs and passwords.

Enterprise – A business venture or company that encompasses one or more factories.

Enterprise Resource Planning (ERP) System –A system that integrates enterprise-wide information including human resources, financials, manufacturing, and distribution as well as connect the organization to its customers and suppliers.

Fieldbus - A category of network that links sensors and other devices to a PC or PLC based controller. Use of Fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network.

Firewall – A device on a communications network that can be programmed to filter information based on the information content, source or destination.

Human Machine Interface (HMI) – The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

Internet – a system of linked networks that are worldwide in scope and facilitate data communication services. The Internet is currently a communications highway for millions of users.

Input/Output (I/O) – a module relaying information sent to the processor from connected devices (input) and to the connected devices from the processor (output).

Light Tower – A device containing series of indicator lights and an embedded controller used to indicate the state of a process based on an input signal.

Local Area Network (LAN) – A network of computers that span a relatively small space. Each computer on the network is called a node, has its own hardware and runs its own programs, but can also access any other data or devices connected to the LAN. Printers, modems and other devices can also be separate nodes on a LAN.

Machine Controller – A control system/motion network that electronically synchronizes drives within a machine system instead of relying on synchronization via mechanical linkage.

Modem – A device that allows a computer to communicate through a phone line.

Management Information System (MIS) – A software system for accessing data from production resources and procedures required to collect, process, and distribute data for use in decision making.

Manufacturing Execution System (MES) – Systems that use network computing to automate production control and process automation. By downloading "recipes" and work schedules and uploading production results, a MES bridges the gap between business and plant-floor or process-control systems.

OPC Client/Server – A mechanism for providing interoperability between disparate field devices, automation/control, and business systems.

Peer-to-Peer network – A networking configuration where there is no server, and computers connect with each other to share data. Each computer acts as both a client (information requestor) and a server (information provider).

Photo Eye – A light sensitive sensor utilizing photoelectric control that converts a light signal into an electrical signal ultimately producing a binary signal based on a interruption of a light beam.

Pressure Regulator – A device used to control the pressure of a gas or liquid.

Pressure Sensor – A sensor system that produces an electrical signal related to the pressure acting on it by its surrounding medium.

Primary Domain Controller – A Windows NT server responsible for managing domain information, such as login IDs and passwords.

Printer – A device which converts digital data to human readable text on a paper medium.

Process Controller – A proprietary, typically rack mounted, computer system that processes sensor input, executes control algorithms and computes actuator outputs.

Programmable Logic Controller (PLC) – A small industrial computer used in factories originally designed to replace relay logic of a process control system and has evolved into a controller having the functionality of a process controller.

Proximity Sensor – A non-contact sensor with the ability to detect the presence of a target, within a specified range.

Redundant Control Server – A backup to the control server that maintains the current state of the control server at all times.

Remote Terminal Unit (RTU) – A computer with radio interfacing used in remote situations where communications via wire is unavailable. Usually used to communicate with remote field equipment. PLCs with radio communication capabilities are also used in place of RTUs.

Servo Valve – An actuated valve whose position is controlled using a servo actuator.

Sensor - A device that senses or detects the value of a process variable and generates a signal related to the value. Additional transmitting hardware is required to convert the basic sensor signal to a standard transmission signal. Sensor is defined as the complete sensing and transmitting device.

Single Loop Controller – A controller that controls a very small process or a critical process.

Solenoid Valve – a valve actuated by an electric coil. A solenoid valve typically has two states: open and closed.

Supervisory Control and Data Acquisition System (SCADA) – Similar to a Distributed Control System with the exception of sub-control systems being geographically dispersed over large areas and accessed using Remote Terminal Servers.

Temperature Sensor – A sensor system that produces an electrical signal related to its temperature and, as a consequence, senses the temperature of its surrounding medium.

Variable Frequency Drive (VFD) – A type of drive that controls the speed, but not the precise position, of a non-servo, AC motor by varying the frequency of the electricity going to that motor. VFDs are typically used for applications where speed and power are important, but precise positioning in not.

Workstation – A computer used for tasks such as programming, engineering, and design.

Wide Area Network – A network that spans a larger area than a LAN. It consists of two or more LANs connected to each other via telephone lines or some other means of connection.

Wireless Device – A device that can connect to a manufacturing system via radio or infrared waves to typically collect/monitor data, but also in cases to modify control set points.

Appendix II

General Threats from the Common Criteria Toolkit

1. Administrative errors of commission (Admin_Err_Commit)
An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

2. Administrative errors of omission (Admin_Err_Omit)
The system administrator fails to perform some function essential to security.

3. Hostile administrator modification of user or system data (Admin_Hostile_Modify)
An administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.

4. Administrator violates user privacy policy (Admin_UserPriv)
An administrator learns the identity (or other privacy related information) of user(s) in violation of user privacy policy. Privacy-related information is sensitive information associated with the identity of a user.

5. A critical system component fails (Component_Failure)
Failure of one or more system components results in the loss of system-critical functionality.

6. Software containing security-related flaws (Dev_Flawed_Code)
A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

7. Failure of a distributed system component (Failure_DS_Comp)
Failure of a component that is part of a distributed system will cause other parts of the distributed system to malfunction or provide unreliable results.

8. Hacker undetected system access (Hack_AC)
A hacker gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

9. Hacker attempts resource denial of service (Hack_Avl_Resource)
A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

10. Hacker eavesdrops on user data communications (Hack_Comm_Eavesdrop)
Hacker obtains user data by eavesdropping on communications lines.

11. Cryptoanalysis for theft of information (Hack_Crypto)
A hacker performs cryptoanalysis on encrypted data in order to recover message content.

12. Hacker masquerading as a legitimate user or as system process (Hack_Masq)
A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process.

13. Message content modification (Hack_Msg_Data)
A hacker modifies information intercepted from a communication link between two unsuspecting entities before passing it on, thereby deceiving the intended recipient.

14. Exploitation of vulnerabilities in the physical environment of the system (Hack_Phys)
A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

15. Social engineering (Hack_Social_Engineer)
A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

16. Malicious code exploitation (Malicious_Code)
An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of system assets.

17. Unexpected disruption of system or component power (Power_Disrupt)
A human or environmental agent disrupts power causing the system to lose information or security protection.

18. Recipient denies receiving information (Repudiate_Receive)
The recipient of a message denies receiving the message, to avoid accountability for receiving the message or to avoid obligations incurred as a result of receiving the message.

19. Sender denies sending information (Repudiate_Send)
The sender of a message denies sending the message to avoid accountability for sending the message or to avoid obligations incurred as a result of sending the message.

20. A participant denies performing a transaction (Repudiate_Transact)
A participant in a transaction denies participation in the transaction to avoid accountability for the transaction or for resulting obligations.

21. Legitimate system services are spoofed (Spoofing)
An attacker tricks users into interacting with spurious system services.

22. Hostile user acts cause confidentiality breaches (User_Abuse_Conf)
A user collects sensitive or proprietary information and removes it from the system.

23. User abuses authorization to collect data (User_Collect)
User abuses granted authorizations to improperly collect sensitive or security-critical data.

24. User errors cause confidentiality breaches (User_Err_Conf)
A user commits errors that cause information to be delivered to the wrong place or wrong person.

25. User error makes data inaccessible (User_Err_Inaccess)
A user accidentally deletes user data or changes system data rendering user data inaccessible.

26. User errors cause integrity breaches (User_Err_Integrity)
A user commits errors that induce erroneous actions by the system and/or erroneous statements its users.

27. User errors undermine the system's security features (User_Err_Slf_Protect)
A user commits errors that cause the system or one of its applications to undermine the system's security features.

28. User's misuse causes denial of service (User_Misuse_Avl_Resc)
A user's unauthorized use of resources causes an undue burden on an affected resource.

29. User abuses authorization to modify data (User_Modify)
A user abuses granted authorizations to improperly change or destroy sensitive or security-critical data.

30. User abuses authorization to send data (User_Send)
A user abuses granted authorizations to improperly send sensitive or security-critical data.

References

1. Roy E. Fraser, Process Measurement and Control - Introduction to Sensors, Communication, Adjustment, and Control, Prentice-Hall, Inc., 2001.

2. Information Security Primer, EPRI Report TR-100797, September 2000

3. Bruce Schneier, Secrets & Lies - Digital Security in a Networked World, John Wiley & Sons, Inc., 2000.

4. Common Criteria Toolbox, Version 6.0f, http://niap.nist.gov/tools/cctool.html.

5. Information Assurance Task Force, Electric Power Risk Assessment, National Security Telecommunications Advisory Committee, http://www.ncs.gov/n5_hp/Reports/EPRA/EPRA.html.

6. Understanding SCADA System Security Vulnerabilities, Riptech, http://www.riptech.com/industry/energy.html

7. Paul Oman et al, Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions, http://www.selinc.com/techpprs/6118.pdf.

8. Common Criteria for Information Technology Security Evaluation, Part1: Introduction and general model, CCIMB-99-031, Version 2.1, 1999.